

新興風險 I: 邊緣 AI 應用規模化挑戰

主題	詳細說明
風險描述	各行業環境中，存在著多樣的人工智慧 (AI)應用情境與技術 (ML, Gen AI..etc). 然而目前大部分仍尚未從 POC 階段轉移到具有明顯投資回報的規模化部署。由於各行業中要求更高的可靠、可管理、安全要求，在技術快速迭代的情況下，邊緣 AI 的普及仍有顯著的困難與內在風險 要能成功地將 AI 在多樣化的產業邊緣環境中，從試驗專案提升到廣泛且可靠的部署，對研華這樣的技術供應商構成了新興且顯著的風險。這些挑戰包括： • 整合與管理複雜性：在大規模且性質各異的邊緣設備中，將多樣化的 AI 模型、各種邊緣硬體與 OT/IT 系統進行可靠整合，加上缺乏成熟的 MLOps 有效管理整個 AI 生命週期，且缺乏一致與可靠的資料來源，皆無法確保高效能與可靠性，這對於邊緣 AI 發展產生重大阻礙。 • 安全與合規負擔：隨著部署規模的擴大，保護分散式邊緣 AI 系統的，並確保符合複雜、不斷演變的全球 AI/資料法規，難度呈指數性增長。 • 技術發展速度與生態系統差距：AI/邊緣技術的快速發展存在技術過時的風險。而生態系統標準和專業技能的差距阻礙了穩健、可互操作解決方案的創建和規模化，並造成人才瓶頸。 • 價值鏈角色模糊與去中介化風險：規模化的複雜性使不同層級的參與者能夠提供更多垂直整合的解決方案，這可能會使無法有效彌合客戶規模化差距的傳統硬體或平台供應商減少價值。
對研華影響	未能有效應對邊緣 AI 規模化挑戰，並協助客戶和合作夥伴克服這些障礙，可能會對研華產生重大影響： • 若無法協助客戶簡化 AI 規模化部署的困難，研華的產品可能不易整合或使用的解決方案不具有競爭力，將會減損硬體價值，或失去價格主導權，從而阻礙營收成長、市佔下降。

	• 由於規模化複雜性，研華的邊緣 AI 部署如可靠度不足或效能不佳，可能會嚴重損害客戶信任以及研華在工業可靠性方面的品牌聲譽。 • 無法有效促進可擴展的 AI 解決方案，會阻礙研華掌握市場先機，搶佔先進邊緣智慧驅動的新市場機會，從而限制在高價值應用領域的擴張。 • 若合作夥伴認為在研華平台上構建和規模化解決方案非常複雜或成本高昂，生態系統的活躍度將會減緩，從而降低市場覆蓋率和失去在邊緣端提供解決方案的領導地位
因應對策	研華策略性地專注於透過提供先進的邊緣運算平台 (WISE-Edge)，以高度軟硬整合協助客戶加快規模化部署、減少投資回報週期。這些工具和生態系統支援，將能協助行業用戶面對工業物聯網邊緣 AI 規模化的挑戰： • 開發賦能平台與解決方案框架： 大力投資 WISE-Edge 平台，以提供統一的管理、硬體抽象、最佳化軟體元件和垂直參考架構，從而簡化可擴展部署並降低風險。 • 建立策略合作夥伴關係與生態系統： 積極與系統整合商、AI 專家、矽晶片供應商和雲端平台合作，以提供更完整、預先整合的解決方案，並駕馭不斷演變的價值鏈。 • 嵌入安全並確保合規準備： 在平台和硬體中構建穩健、可擴展的安全功能，並主動設計以符合與大規模工業部署相關的新興全球 AI 和資料法規。 • 增強內部能力與人才發展： 投資於內部培訓計畫、跨職能團隊發展和策略性招聘，以建立支援客戶和開發可擴展解決方案所需的專業、整合技能組合 (AI、MLOps、邊緣軟體、安全性、領域知識)。 • 加強客戶與合作夥伴賦能： 提供全面的培訓、文件、可擴展的支援模型，以及可能專門針對指導客戶應對大規模部署和管理邊緣 AI 解決方案挑戰的專業服務

新興風險 II: 自主式 AI 代理技術衍生之營運與人才風險

主題	詳細說明
風險描述	自主式 AI 代理 (Agentic AI Agent) 技術於 2025 年崛起，成為最先進之 AI 代理解決方案。其可自主規劃、產生並執行任務，與過往之 AI 代理技術有本質上之差異。公司若未能即時將此類最新 AI 技術導入內部營運，並同步養成及取得相關人才，將影響營運效率與組織競爭力。主要挑戰包括： • 算力架構與成本管理複雜度：新技術使 token 消耗量大幅增加，需要具備管理地端運算伺服器叢集新技能之人才，以合理成本確保足夠算力。此類人才市場稀缺，須透過正確管道招募並妥善留任，同時亦須由內部培育養成。 • AI 代理管理模式轉變：自主式 AI 代理會自動產生任務並自動執行，需要與以往截然不同之管理方法。AI Harness (AI 代理管控框架) 成為重要課題，須招募及培育具備該能力之人才，確保代理行為安全、可控且可稽核。 • 業務轉型思維：自主式 AI 代理須由 AI 工程師與業務使用者共同定義。公司需要具備正確轉型思維之業務人員；於外部招募此類人才不易，須透過培訓計畫由內部養成。 • 多代理串連與協作：隨著自主式 AI 代理數量持續增加，須將各代理互相串連協作，需要具備新型態 AI 代理串連技能之員工。 • 資料治理與資安：自主式 AI 代理需廣泛存取內部系統與資料，權限管理、資料安全與機密保護之複雜度大幅提高，需具備 AI 資安治理能力之人才。 • 技術快速迭代風險：近期內可能再出現另一種新型態之 AI 代理技術。公司須擁有能快速學習新 AI 技術之人才，確保持續跟上最新技術發展。

對研華影響	• 營運效率落後：若競爭對手率先以自主式 AI 代理精實內部流程，其成本與速度優勢將削弱研華之營運競爭力。 • 人才缺口影響導入時程：無法招募或留任具備算力叢集管理、AI Harness、多代理串連等新技能之人才，將使 AI 導入時程延宕，營運效率提升受限。 • AI 治理失控風險：自主式 AI 代理若未受妥善管控，可能自動執行錯誤任務、產生錯誤決策或不當存取資料，造成營運中斷、資料外洩或合規風險。 • 成本失控風險：token 消耗大幅增加，若無妥善算力策略與成本管理，AI 導入成本可能超出效益。 • 組織轉型受阻：業務人員若缺乏正確轉型思維，AI 僅停留於單點工具而無法規模化，組織競爭力與對新世代人才之吸引力同步下降。
因應對策	• 建立 AI Harness 框架：制定自主式 AI 代理導入藍圖、管控標準 (AI Harness)、權限與稽核機制，確保 AI 代理安全可控。 • 算力基礎建設與成本管理：規劃地端運算伺服器叢集與混合雲算力策略，以合理成本確保足夠算力；招募並培育具備算力叢集管理能力之人才。 • 策略性人才招聘與留任：定義關鍵新職能 (如 AI 基礎設施工程師、AI Harness 工程師)，透過正確管道 (專業獵才、技術社群、產學合作) 進行招募，並以具競爭力之薪酬與激勵機制留任稀缺人才。 • 內部人才培育與轉型：透過培訓計畫 (如研華學院 AI 課程、實作專案) 培養業務人員正確之 AI 轉型思維，並培育內部工程人才之新型 AI 代理技能。 • 業務與 AI 共創機制：建立 AI 工程師與業務使用者共同定義自主式 AI 代理之機制，由試點到規模化推廣，確保 AI 導入貼合業務需求並產生實質效益。 • 持續技術偵測與快速學習：建立技術雷達與外部夥伴 (AI 供應商、學研機構) 合作機制，培養能快速學習新 AI 技術之人才，確保公司即時掌握並導入新一代 AI 代理技術。

